Awair GB Limited
Data Controller

Document Version 3.1

Data Audit: 20 February 2025

ICO REGISTRATION NO: ZB 518584

C O R P O R A T E
R E S P O N S I B I L I T Y:-

ANDREA FACCHINI

Data Protection Manager

BUSINESS COMPLIANCE DOCUMENT

AWAIR GB LIMITED

DATA PROTECTION ACT 2018

UK - GENERAL DATA PROTECTION REGULATIONS –

PRIVACY & ELECTRONIC COMMUNICATIONS REGULATIONS 2003

Incorporating proposals from the Data Access & Use Bill 2025

©TransitionLaw2025

Contents by Section

PART ONE – BUSINESS OPERATIONAL POLICIES

PART TWO – DATA CONTROL POLICIES

PART THREE – PROCEDURAL POLICIES

©TransitionLaw2025

PART FOUR – DATA RIGHTS & BREACH POLICIES

PART FIVE – LEGITIMATE INTEREST & UPDATES POLICIES

©TransitionLaw2025

Business Compliance Document

PART ONE of FIVE

BUSINESS OPERATIONAL POLICIES

©TransitionLaw2025

1 Company Contact Details

1.1 Awair GB Limited 64 Southwark Bridge Road, London. SE1 0ES hereinafter referred to as 'the Company', We, Us and Our.

1.2 Our email address is: andrea.facchini@awair.eu

1.3 We are a Data Controller under the provisions of the UK GDPR and the Data Protection Act 2018 and have registered with the UK Information Commissioners office:

ICO Registration Number: ZB 518584

2 Status of key personnel

2.1 We have designated **Mr Andrea Facchini** as **Data Protection Manager** for the business.

2.2 We are not required to formally designate a Data Protection Officer (DPO) Because we are not engaged in any of the following activities:

2.2.1 We are not a public authority.

2.2.2 We are not an organisation that carries out the regular and systematic monitoring of individuals on a large scale.

2.2.3 We are not an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions.

2.3 We do not believe it is necessary to appoint a DPO voluntarily but if this policy changes, or such a change is made or planned to be made, we will complete a Data Protection Impact Assessment and update this policy statement accordingly.

3 Introduction and Overview

3.1 The Company is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

3.2 This policy document has been prepared in view of the Retained Regulation (EU) 2016/679, which is now assimilated law in the UK, in accordance with section 5 of the Retained EU Law (Revocation and Reform) Act 2023.

3.3 Pursuant to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) the Company must:

3.3.1 use technical or organisational measures to ensure personal data is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;

3.3.2 implement appropriate technical and organisational measures to demonstrate that it has considered and integrated data compliance measures into the Company's data processing activities; and be able to demonstrate that it has used or implemented such measures and complied with the data protection principles.

3.3.3 The Company maintains records of its own actions and our interactions with other Data Controllers and our Data Processors to ensure we can suitably demonstrate

©TransitionLaw2025

adherence to the data protection principles. Specifically, we ensure data is processed:

(a) Fairly, Lawfully and Transparently.

(b) for limited purposes.

(c) in a manner which is adequate, relevant and not excessive.

(d) in a manner which is accurate and not kept for longer than necessary.

(e) in accordance with the prescribed rights.

(f) for no longer than necessary.

(g) in a manner which is secure and not transferred to countries outside the UK, without appropriate safeguards.

(h) in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4 **The purpose of this policy is to:**

4.1 protect against potential breaches of confidentiality;

4.2 ensure all our data assets and IT facilities are protected against damage, loss or misuse;

4.3 support the Company's aims in ensuring all staff are aware of and comply with UK law and the Company's procedures applying to the processing of personal data; and

4.4 increase awareness and understanding within the Company of the requirement for information security and our responsibility to protect the confidentiality and integrity of the data we handle.

5 Definitions

For the purposes of this Policy:

Staff	means the Directors and staff members of the Limited Company to which this policy applies, whether such staff are retained on Pay-As-You-Earn contracts, zero hour contracts or act as volunteers to the organisation and; temporary and agency workers, other contractors, interns, volunteers and apprentices; and Self-employed data processors engaged under contract to the Company and to the extent permissible under the law includes their agents, employees and representatives as appropriate.

©TransitionLaw2025

business information	means business-related information other than personal information regarding customers, clients, suppliers and other business contacts of the Company;
Company information	means personal data relating to staff, customers, clients and suppliers; and Any other business information; and Confidential information. (see below).
Confidential information	means trade secrets or other confidential information (either belonging to the Company or to third parties) that is processed by the Company;
personal data	means data relating to an individual who can be identified (directly or indirectly) from that data; Personal data is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, e.g. their name, identification number, location data or online identifier.
pseudonymised	means the process by which personal data is processed in such a way that it cannot be used to identify an individual without the use of additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable individual;
special category data	means personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic data, biometric data (where used to identify an individual) and data concerning an individual's health, sex life or sexual orientation.

©TransitionLaw2025

6 Roles and responsibilities

6.1 We consider that Information security is the responsibility of all staff. However, the Company's **Data Protection Manager** has particular responsibility for:

6.1.1 monitoring and implementing this policy;

6.1.2 monitoring potential and actual security breaches;

6.1.3 ensuring staff are aware of their responsibilities by providing suitable training; and

6.1.4 ensuring compliance with the requirements of the UK GDPR as assimilated law and other relevant legislation and guidance.

7 Scope of the Policy

7.1 The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Company, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

7.2 This policy applies to all staff, who should act on and interpret this policy in both the letter and the spirit of the applicable law.

7.3 All staff must be familiar with this policy and comply with its terms.

7.4 The Company information covered by this policy includes Confidential information.

7.5 This policy has been drafted with care to ensure that it is clear and easy to understand.

7.6 We will review and update this policy regularly in accordance with our data protection and other obligations.

7.7 We may amend, update or supplement the policy at any time.

7.8 We will circulate any new or modified policy when it is adopted.

8 General principles of data protection

8.1 All Company information must be treated as commercially valuable and protected from loss, theft, misuse or inappropriate access or disclosure.

8.2 Personal data, and special category data, must be protected against unauthorised and/or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical and organisational measures.

8.3 Staff should discuss with line managers the appropriate security arrangements and technical and organisational measures which are appropriate and in place for the type of information they access in the course of their work.

8.4 Company information (other than personal data) is owned by the Company and not by any individual or team.

©TransitionLaw2025

8.5 Company information must be used only in connection with work being carried out for the Company and not for other commercial or personal purposes;

8.6 Personal data must be used only for the specified, explicit and legitimate purposes for which it is collected.

9 Information management

9.1 Personal data must be processed in accordance with:

9.1.1 the data protection principles, set out in this data protection policy;

9.1.2 this data protection policy generally; and

9.1.3 all other relevant Company policies.

9.2 In addition, all information collected, used and stored by the Company must be:

9.2.1 adequate, relevant and limited to what is necessary for the relevant purposes;

9.2.2 kept accurate and up to date;

9.3 The Company will take appropriate technical and organisational measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage, including:

9.3.1 pseudonymisation of personal data where necessary;

9.3.2 encryption of personal data. e.g. for onward transmission by email;

9.4 Personal data and confidential information will be kept for no longer than is necessary and stored and destroyed in accordance with the Company's records retention policy.

10 Lawfulness of processing

10.1 There are 6 lawful bases for data processing.

10.2 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues, review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing.

10.3 The lawful bases for data processing are as follows:

10.3.1 **Consent:** Where we process information with the specific consent of the individual concerned, whether for our services or for referral to our professional partners.

10.3.2 **Contract:** The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the direct request of the data subject prior to entering into a contract.

10.3.3 **Legal Obligation:** The processing is necessary for a compliance with a legal obligation to which the Controller is subject.

©TransitionLaw2025

10.3.4 **Vital Interests:** The processing is necessary in order to protect the vital interests of the data subject or of another natural person.

10.3.5 **Public Task:** The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

10.3.6 **Legitimate Interests:** The processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

10.4 Except where the processing is based on consent, we shall satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose); and

10.4.1 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

10.4.2 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

10.4.3 where 'special category data is processed, also identify a lawful special condition for processing that data and document it; and

10.4.4 if criminal records data are processed, also identify a lawful condition for processing that data, and document it.

10.5 When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:

10.5.1 conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

10.5.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

10.5.3 keep the LIA under review, and repeat it if circumstances change; and

10.5.4 include information about our legitimate interests in our relevant privacy notice(s).

Special Category Data

10.6 Some Personal Data needs additional care and security this is Special Category data, sometimes referred to as 'sensitive personal data' or 'sensitive personal information'.

10.7 Special Category Data means personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic data, biometric data (where used to identify an individual) and data concerning an individual's health, sex life or sexual orientation.

10.8 The Company may from time to time need to process special category data. We will only process special category data if:

©TransitionLaw2025

10.8.1 we have a lawful basis for doing so as set out above; and

10.8.2 one of the special conditions for processing special category data applies:

(a) the data subject has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(d) processing relates to personal data which are manifestly made public by the data subject;

(e) the processing is necessary for the establishment, exercise or defence of legal claims; or

(f) for reasons of substantial public interest; or

(g) for the purposes of preventive or occupational medicine.

10.9 Where we deal with Special Category data for our employees, our subsidiary legal bases for employees are described in the Human Resources section of this document.

10.10 When we deal with Special Category data for clients the lawful bases are those provided for in Article 9(2) of the UK GDPR which are assessed on a case-by-case basis.

11 Data Access Rights

11.1 Our **Data Protection Manager** can be contacted for the following data access reasons: -

11.1.1 To obtain a copy of the Personal Data we hold about an individual.

11.1.2 If someone believes any Personal Data or information we hold about them is incorrect or incomplete. Any information or data which is found to be incorrect will be corrected as soon as possible.

11.1.3 To have an individual's personal data removed entirely from our systems.

11.1.4 To make a request regarding Data Portability or any other rights under the data protection legislation.

11.1.5 Data Access is usually free of charge. As soon as we are satisfied as to the identity of the person making the request, we will send them, within a month of the request a copy of the Personal Data we hold relating to them.

11.1.6 As soon as we are satisfied as to the identity of the person making a removal request and the data is not required to be kept for any other lawful reason or purpose it will be removed from our systems forthwith.

11.1.7 As soon as we are satisfied as to the identity of the person making a rectification request the data in question will be corrected or rectified as appropriate in our systems forthwith.

11.2 Data Subjects have rights of access to the data we hold about them. Requests to exercise these rights should be directed to our **Data Protection Manager**.

©TransitionLaw2025

11.3 Further information about handling a DSAR is available in our Data Subject Access Request Policy in this document.

12 Data Protection Impact Assessments (DPIAs)

12.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the Company is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

12.1.1 whether the processing is necessary and proportionate in relation to its purpose;

12.1.2 the risks to individuals; and

12.1.3 what measures can be put in place to address those risks and protect personal data.

12.2 Before any new form of technology is introduced, the **Data Protection Manager** will assess whether a DPIA should be carried out.

13 Practical Data Protection Actions

13.1 Given the internal confidentiality of personnel files, access to such information is limited to the specifically authorised staff and management on a necessity basis. Except as provided in individual roles, other staff are not authorised to access that information.

13.2 All staff must keep personnel information strictly confidential.

13.3 Staff may ask to see their personnel files and any other personal data in accordance with the UK GDPR and other relevant legislation. For further information, see the Company's data subject access request policy.

Access to premises and information

13.4 Office doors, keys and access codes must be kept secure at all times and keys or access codes must not be given or disclosed to any third party at any time.

13.5 Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by, e.g. through office windows or during video conference calls.

13.6 At the end of each day, or when desks are unoccupied, all paper documents, backup systems and devices containing confidential information must be securely locked away.

Computers and IT

13.7 Password protection and encryption must be used where available on Company computers and systems in order to maintain confidentiality.

13.8 Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis. Passwords must not be written down or given to others.

13.9 Computers and other electronic devices must be locked when not in use and when you leave your desk, to minimise the risk of accidental loss or disclosure.

©TransitionLaw2025

13.10 Confidential information must not be copied onto floppy disk, removable hard drive, CD or DVD or memory stick/ thumb drive without the express permission of a manager.

13.11 Data held on any of these temporary devices should be transferred to the Company's computer(s) and/or network as soon as possible in order for it to be backed up and then deleted from the device.

13.12 All electronic data must be securely backed up in accordance with the Company approved back up schedule.

13.13 Staff must ensure they do not introduce viruses or malicious code on to Company systems.

13.14 Software must not be installed or downloaded from the internet without it first being virus checked. Staff should contact their line manager for guidance on appropriate steps to be taken to ensure compliance.

Communications and transfer of information

13.15 Care must be taken about maintaining confidentiality when speaking in public places, e.g. when speaking on a mobile telephone.

13.16 Confidential information must be marked 'confidential' and circulated only to those who need to know the information in the course of their work for the Company.

13.17 Confidential information must not be removed from the Company's offices unless required for authorised business purposes.

13.18 Where confidential information is permitted to be removed from the Company's offices, all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained. Staff must ensure that confidential information is:

13.18.1 stored on an encrypted device with strong password protection, which is encrypted at rest and kept locked when not in use;

13.18.2 when in paper copy, not transported in see-through or other unsecured bags or cases;

13.18.3 not read in public places (e.g. waiting rooms, cafes, trains); and

13.18.4 not left unattended or in any place where it is at risk (e.g. in conference rooms, motor vehicles, public transport or cafes).

Email and cloud storage accounts

13.19 Postal and email addresses and numbers should be checked and verified before information is sent to them.

13.20 Particular care should be taken with email addresses and attention paid to avoid opportunities for auto-complete features to insert incorrect addresses.

13.21 All sensitive or particularly confidential information should be encrypted before being sent by email.

©TransitionLaw2025

13.22 Further details regarding data security and how documents and emails should be protected are set out in the Company's data security, transfer, storage and retention policy.

13.23 Staff members must not use a personal email account or cloud storage account for work purposes.

Data Transfer to third parties

13.24 Third parties should be used to process Company information only in circumstances where appropriate written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings. Consideration must be given to whether the third parties will be processors for the purposes of Article 28, UK GDPR.

13.25 Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the **Data Protection Manager** for advice and more information.

Data Protection Training

13.26 All staff will receive training in data protection. New joiners will receive training as part of the induction process. Further training will be provided annually or whenever there is a substantial change in the law or our policy and procedure.

13.27 The **Data Protection Manager** will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or our Information management and security policy or procedures, please contact the **Data Protection Manager**.

Reporting Data Subject Access Requests (DSARs)

13.28 All members of staff have an obligation to report actual or suspected Data Subject Access Requests (DSARs). This allows the Company to:

13.28.1 Respond to the request as required by law; and

13.28.2 maintain a register of requests;

13.29 Please refer any suspected DSAR to the **Data Protection Manager** for immediate action.

Reporting data breaches

13.30 All members of staff have an obligation to report actual or potential data protection compliance failures. This allows the Company to:

13.30.1 investigate the failure and take remedial steps if necessary;

13.30.2 maintain a register of compliance failures; and

13.30.3 make any applicable notifications.

13.31 Please refer any suspected data breach to the **Data Protection Manager** for immediate action.

©TransitionLaw2025

14 International data transfers

14.1 There are stringent legal restrictions on international transfers of personal data and transfers to international organisations.

14.2 Staff may only transfer personal data outside the UK, or to an international organisation, with the prior written authorisation of the **Data Protection Manager**

14.3 We do not generally operate outside of the United Kingdom but we may maintain professional contacts in other countries.

14.4 All Data and information collected in any State will be processed in the UK.

14.5 Due to the operation of the Internet and other computer based applications Personal Data under our control may transit countries outside of the UK.

14.6 We will only transfer data outside the UK if adequate safeguards are in place in the destination country.

14.7 The Main Establishment for all of our Data Processing is the UK.

14.8 The lead supervisory authority is UK Law and the UK Information Commissioners Office whose address is Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

14.9 We have considered the requirements of Article 27 UK GDPR and decided that we do not need to appoint an EU Representative because

14.9.1 We are not a public authority; and

14.9.2 our international processing is only occasional, of low risk to the data protection rights of individuals; and

14.9.3 does not involve the large-scale use of special category or criminal offence data.

©TransitionLaw2025

Business Compliance Document

PART TWO of FIVE

DATA CONTROL POLICIES

©TransitionLaw2025

15 Personal Data under our control

15.1 Data under control analysis chart

Personal Data	Lawful Base(s)	Types of Data	Retention Period	Data Sharing
Prospective and existing Clients providing their personal information either Online or Offline including Social Media, telephone and by written means to ourselves or third parties to request information regarding our available products and services	**Consent**	Identity Data Marketing Data Communications Data	Maximum of 12 months. Or Until Consent is withdrawn whichever comes first.	Data is only shared with our authorised Data Processors.
Clients providing their information for the purposes of contracting with us for goods and services. We process this Personal Data to provide relevant advice, to manage and administer our business relationships and communicate with clients, their employees and representatives, to manage billing and payments and to keep records.	**Contract**	Identity Data Financial Data Transaction Data Marketing Data Communications Data	Duration of Contract Plus Seven Years	Data is shared with our Data Processors and our professional advisors including IT, Accounts and Legal where necessary.
Personal data provided because the Data Subject may be interested in working with us or learning more about working with us.	**Consent**	Identity Data	Time to consider request. Maximum of 12 months; or Until Consent is withdrawn whichever comes first.	Data is only shared with our authorised Data Processors.

©TransitionLaw2025

Personal Data	Lawful Base(s)	Types of Data	Retention Period	Data Sharing
Online or Offline face to face meetings with people who provide their personal data to us for the purposes of later contact regarding products and services provided by us.	**Consent**	Identity data	Maximum of 12 months. Or Until Consent is withdrawn whichever comes first.	Data is only shared with our authorised Data Processors.
Suppliers of products and services to us who provide information of themselves or individuals who assist them to provide us with products and services on their behalf.	**Contract**	Identity data Transaction Data	Duration of Contract Plus Seven Years	Data is shared with our Data Processors and our professional advisors including IT, Accounts and Legal where necessary.
Personal Data of prospective customers provided by third parties for future contact by us regarding our products and services.	**Consent**	Identity data	Maximum of 12 months. Or Until Consent is withdrawn whichever comes first.	Data is only shared with our authorised Data Processors.
Suppliers of software who manage data via End User Service Agreements (EUSAs).	**Contract**	Identity Data Transaction Data Technical Data	Duration of Contract Plus Seven Years	Data is only shared with our authorised Data Processors.
Employees who provide their personal information for the purposes of working with us.	**Contract** **Legal Obligation**	Special Category Data Identity Data Technical Data	Duration of Contract Plus Seven Years Any Other Legal Requirements	Data is shared with our Data Processors and our professional advisors including HMRC, IT, Accounts and Legal where necessary.

©TransitionLaw2025

Personal Data	Lawful Base(s)	Types of Data	Retention Period	Data Sharing
People identified via proprietary Video Conference software	**Legitimate Interests**	Identity Data	Until Legitimate Interest no longer exists or 3 months if recorded	Data is only shared with our authorised Data Processors

16 Data Sharing with others

16.1 Below is a chart showing all the organisations and individuals with whom we may share data.

Processor	Processor
Google AWS	**Hubspot**
Microsoft Teams	
Zoom	
Social Media: Linkedin/WhatsApp FB/Tik Tok/Twitter/Snapchat/Instagram	
Mailchimp	
AI – ChatGPT/CoPilot/Fireflies	

17 Types and Categories of Personal Data

17.1 **Identity data:** name, username, title, date of birth. Contact data: billing and delivery address, email address, phone number.

17.2 **Financial data:** payment card details (processed by a third-party payment services provider and not stored by us).

17.3 **Transaction data:** details of products purchased, amounts, dates etc.

17.4 **Technical data:** IP address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform based on your Cookie preference choices.

17.5 **Profile data:** username and password, purchases or orders made by users.

17.6 **Usage data:** information about how users use our website, products and services.

17.7 **Marketing and communications data:** record of Website users preferences in receiving marketing from us about the products we sell.

©TransitionLaw2025

18 Consequences of failing to provide Personal Data

18.1 Generally, if you fail or refuse to provide us with your Personal Data we will not be able to deal with your enquiry or do business with you.

18.2 The following paragraphs explain the consequences for each Lawful Basis of processing:

18.2.1 Consent: It is your decision to provide your information by consent. We protect your data as described in this document but we cannot proceed with an enquiry without, for example your contact details to receive a reply.

18.2.2 Contract: We cannot contract with you for goods or services in business unless you provide us with, at least some of your details. We adhere to the principle of Data Minimisation and only collect enough data to complete the task at hand.

18.2.3 Legal Obligation: If we have a legal obligation to process your data, failure to provide the necessary information may have adverse consequences for you. If this is the case we will tell you.

18.2.4 Public Task: If we are required to process your personal data in the public interest or the exercise of official authority we will inform you. Failure to provide data under these circumstances will mean we cannot include you in the processing activity.

18.2.5 Vital Interests**:** If data processing is required to protect the vital interests of a natural person then it is likely we will be in possession of the data before the need arises. If you have not provided us with your data this situation cannot apply to you.

18.2.6 Legitimate Interests: Where data processing occurs and has been deemed to be in our legitimate interests this will be based on a written assessment of need. There is usually no need for the data subject to provide their data for this purpose, although you do have the right to object to its use under certain circumstances but you usually must provide some identification data to make such an objection.

19 Data Storage, transfer and retention

19.1 We recognise the need for structural and organisational data security and have included such measures within our data protection systems by design. The following policies deal with our forward planning and organisational security arrangements.

Data Transfer

19.1.1 Personal Data under our control will only be transferred to a third party organisation under the terms of a written Data Processing or data sharing contract and where we have received sufficient guarantees of safeguards from them as Data Controllers in their own right.

19.1.2 Personal Data sent by email will be encrypted where possible, where it is not possible the email itself should be encrypted**.** Attachments to emails containing Personal Data will always be encrypted.

19.1.3 Personal data will not be transferred over a wireless network if a hardwired network is available.

©TransitionLaw2025

19.1.4 Where it is necessary to transfer the password or encryption code for an email it will not be transferred with the encrypted email.

19.1.5 Passwords if transferred by email will be sent over a different email system to that of the encrypted email. Where this is not possible another means will be considered E.g. Voice or SMS transfer.

19.1.6 SMS transfers of Personal Data will be kept to an absolute minimum and only sent to telephone numbers which have previously been satisfactorily identified as the correct recipient, ideally after a confirmatory voice call on that particular line.

19.1.7 Transfer of hard copy documents containing Personal Data will be achieved through personal physical transfer or if using the Royal Mail system by Special Delivery only. We will not use Recorded Delivery/'Signed For' under any circumstances.

19.1.8 Personal Data contained on removable media must be encrypted and its transfer achieved through personal contact or if using Royal Mail by Special Delivery only.

19.1.9 Particular attention and special care will be taken when transporting Personal data offsite. Such as transporting removable media and computers for homeworking. Confirmation should be made prior to such activity that the device is encrypted at rest.

Data Storage

19.1.10 Personal Data is held by us in secure electronic devices such as computers, Ipads, mobile phones and separate back up devices, computers and Internet Cloud based servers.

19.1.11 Data is also held by us in paper form in files relating to individuals, which are secured by restricted access protocols and by virtue of the physical security at their location.

19.1.12 We have no plans to introduce new technology such as face recognition, biometrics or fingerprint recognition into our Data processing activities but if such a change is made or planned to be made We will complete a Data Protection Impact Assessment and update this policy statement.

19.1.13 Hard copies of Personal Data will be kept securely in a locked room or area, a locked cupboard or secure filing system.

19.1.14 Removable Media containing Personal Data are kept securely in a locked cupboard or secure filing system.

19.1.15 We will retain the data of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

19.1.16 Details of retention periods for specific data is provided in the data under control analysis chart above.

19.1.17 For repeat clients or those with additional or repeating expectations, their data will be kept until the expectations no longer exist plus 7 years.

19.1.18 Where we have a legal obligation to retain data outside of these periods they will be held securely and reviewed regularly until the obligation no longer exists.

©TransitionLaw2025

20 Individuals Data Rights

20.1 We protect the individual's rights provided by the UK GDPR and Data Protection Act 2018 as being the following:

20.1.1 The right to be informed (Confirmation processing is taking place or not.)

20.1.2 The right of access

20.1.3 The right to rectification

20.1.4 The right to erasure

20.1.5 The right to restrict processing

20.1.6 The right to data portability

20.1.7 The right to object

20.1.8 The right not to be subject to automated decision making, including profiling.

20.2 Under the UK General Data Protection Regulation (UK GDPR) and The Data Protection Act 2018 (DPA) Data Subjects have a number of rights with regard to their personal data.

20.2.1 These rights are protected by design and default in our data protection systems.

20.2.2 To exercise any of their rights Data Subjects should contact our **Data Protection Manager** using the details given above.

20.2.3 In our Online presence and Website we provide a method for contacting us and requesting Access to any data held by ourselves subject to the usual legal controls.

20.3 In the event Data Subjects provide their data directly to us for the purpose of a contract, or in circumstances where it is provided by consent, Data Subjects have the right to be provided with their data in a structured, machine-readable format.

20.4 Following a request relating to Data Portability we will transmit the relevant personal data to the data subject or their nominated data controller where it is possible and technically feasible for us to do so.

20.5 Where data has been provided by Consent there is a right to withdraw the Consent at any time. However, withdrawal of Consent does not affect the lawfulness of any processing of the data based on the Consent prior to its withdrawal.

20.6 Where we need to process data for the purposes of entering into a Contract with a Data Subject, failure to provide such data it may mean that we cannot establish legal relations between ourselves and the Data Subject and the contract may not be able to go ahead. We will inform the Data Subject if this happens.

20.7 Automated decision making and profiling means making decisions without human intervention, usually with the use of a computer program or software. We may use automated decision making about you if it is necessary for entering into or performing a Contract with you or where you Consent to the actions.

©TransitionLaw2025

20.8 We will retain and use Data Subjects personal information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. If we need to use the data for a reason it was not collected and the Data Subject is not aware of this, we will inform them and in appropriate cases obtain further consent to such use.

20.9 Where we have not obtained the data personally from the Data Subject, we must provide them with the information described in this Privacy Notice and some additional information.

20.10 The additional information must be provided at least by the time we contact the Data Subjects and in any event within the space of one month after we obtain it.

20.11 If our processing is based on Legitimate Interests, the Data Subjects are entitled to know what and whose Legitimate Interests they are.

20.12 The Data Subjects are entitled to know the purpose of the processing, whether we or someone else is processing it and the categories of Personal Data involved.

20.13 The Data Subjects are entitled to know the source of the information and whether the source is publicly accessible.

20.14 There are some exceptions to this additional information rule. If we obtain Personal Data from a source other than the Data Subjects, the additional information rules will apply unless:-

20.14.1 They already have the information regarding our processing; or

20.14.2 It would take a disproportionate effort or be impossible to provide them with it; or

20.14.3 They are already legally protected under separate provisions; or

20.14.4 We have a legal duty not to disclose it.

20.15 Data Subjects have the right to complain to the Data Regulator at the Information Commissioners Office on 0303 123 1113 or through their website www.ico.org.uk

21 Children's Personal Data

21.1 We do not contract with children to provide products or services.

21.2 We have considered the provisions of the Age Appropriate Design Code (AADC) and concluded we are not a relevant ISS likely to be accessed by children pursuant to Section 123 Data Protection Act 2018.

21.3 We may record details of client's children if relevant and appropriate to our business activity or for the purposes of giving the client advice and we may subsequently reference the children in our records.

21.4 In all cases where a child is under 13 years, we will obtain parental consent for the transaction and their consent to record the child's details in our records.

21.5 If a Parent or Guardian of a person under 13 years of age discovers their child has engaged with our Website without their consent, please inform us immediately using the contact email address provided above.

©TransitionLaw2025

21.6 There is nothing on our Website which could be damaging to children who view the pages or the pictures. Our Products and Services are not made available to children under 18 years.

21.7 The products on our Website are only available and relevant to adults over the age of 18 years.

21.8 We protect the rights of the child in accordance with the UNCRC by trading only with Adults.

22 Business Sale or Transfer of Ownership provisions

22.1 In the event our business, or part of it, is taken over, bought or merged with another business we may need to disclose any personal data we are holding to the other Company so they can continue to provide services to the data subject(s), post-sale, in accordance with this or other Privacy Policy systems..

22.2 It may also be necessary to transfer personal data under our control to a Company that is negotiating with us for the purchase of our business but only where it is necessary to evaluate the business purchase transaction.

22.3 In the case of a pre-sale transfer of personal data, the data would be kept safe during the negotiations and destroyed by the third party if the sale or merger did not go ahead.

©TransitionLaw2025

Business Compliance Document

PART THREE of FIVE

PROCEDURAL POLICIES

©TransitionLaw2025

23 Human Resources and Payroll

23.1 As a core activity within our business We process data for the purposes of our Human Resources function and Payroll function.

23.1.1 The lawful authority we rely on for processing this personal data is article 6(1)(b) of the UK GDPR, which relates to processing necessary to perform a contract or to take steps as requested, before entering a contract.

23.1.2 The lawful authority we rely on to process any information provided as part of an employment application which is special category data, such as health, religious or ethnic information is Article 9(2)(b) of the UK GDPR, which also relates to our obligations in employment and the safeguarding of the employee's fundamental rights and article 9(2)(h) for assessing an individual's work capacity as an employee.

23.1.3 Also, Schedule 1 part 1(1) and (2)(a) and (b) of the Data Protection Act 2018 which relates to processing for employment, the assessment of working capacity and preventative or occupational medicine.

23.1.4 We recognise that staff are entitled to the same data access rights listed above and should follow the procedure laid out in the Subject Access Requests section of this policy document.

Recruitment

23.1.5 We use the information provided during the recruitment process to progress employment applications with a view to offering an employment contract.

23.1.6 We use contact details provided to contact applicants to progress their application and the other information provided to assess suitability for the role.

23.1.7 We do not collect more information than we need to fulfil our stated purposes and will not keep it longer than necessary.

23.1.8 If an individual is invited for interview we may ask for additional information such as personal referees and health information to establish fitness to work.

23.1.9 If we make a conditional offer of employment, we will ask for information so that we can carry out pre-employment checks. An individual must successfully complete pre-employment checks to progress to a final offer.

23.1.10 We must confirm the identity of our staff and their right to work in the United Kingdom and seek assurance as to their trustworthiness, integrity and reliability.

Payroll Matters

23.1.11 To manage our Payroll function we use information provided by employees to ensure accurate and timely payment of wages and emoluments.

23.1.12 The lawful authority for this function is our contractual relationship with employees and the legal obligation we have under HMRC and other legislation.

23.1.13 We collect no more information than is necessary to perform the function.

©TransitionLaw2025

23.1.14 We may complete the Payroll function ourselves or contract with a Data Processor to perform the function on our behalf, in which case the information transmission between ourselves and the Data Processor will be subject to strict security measures, contractual terms and encrypted where necessary and appropriate.

24 Home Working Policy

Introduction

24.1 This policy covers processing of Personal data and the use of electronic devices which could be used to access the Company's systems and store information, alongside employees' own personal data. Such devices include, but are not limited to, smart phones, tablets, laptops and similar technologies.

24.2 The Company is the Data Controller of any Personal Data processed on its behalf and remains in control of the data regardless of the ownership of the device, or the location in which the data is processed.

24.3 All employees or approved contractors of the Company are required to keep any company information and data securely and comply with Data Protection law.

24.4 All employees or approved contractors are required to assist and support the Company in carrying out its legal and operational obligations, including co-operating with the management team should it be necessary to access or inspect company data stored on your personal device or equipment at your home.

24.5 The Company reserves the right to refuse, prevent or withdraw access or permissions for users to work from their homes and/or particular devices or software where it considers there are unacceptable security, or other risks, to its employees, business, reputation, systems or infrastructure.

Security and Confidentiality of Materials

24.6 All employees or approved contractors must follow The Company policies and procedures in relation to working with personal data as if they are present in the office.

24.7 There are also additional risks relating to working remotely. All employees or approved contractors must adhere to these instructions and follow both the spirit and the letter of this policy as this list of potential risks is not an exhaustive one.

24.8 The data protection principles still apply and need to be adhered to, i.e. you should only access as much personal data as you need for the task at hand.

24.9 You must consider "appropriate security", both at home and in transit. Additionally, you must be able to provide evidence you are complying with these principles on request.

24.10 Do not leave a computer with personal confidential information on screen. An unauthorised person reading personal data is a data breach.

24.11 Do not leave your computer 'logged on' when unattended. Think about who may access the device when you are not around – whether deliberately or accidentally.

24.12 Make sure rooms containing computers and other equipment, are secure when unattended, with windows closed and locked and blinds or curtains closed.

©TransitionLaw2025

24.13 When making a business phone or online conference call remember that it is confidential and consider who is around who might overhear.

24.14 Levels of Home Security and access to Personal Data should be the same as at work.

24.15 Work should only be completed on Company approved systems and applications.

24.16 Do not hold Personal Data on personally owned electronic devices. (i.e. Devices not provided by the Company) unless approved in writing by the Company.

24.17 Any Company Personal Data downloaded to a personal device must be deleted as soon as possible.

24.18 If using a personally owned device, check for automatic uploads to Cloud storage systems. E.g. If subscribed to iCloud or Dropbox, you may inadvertently be uploading Company documents to your personal account in these applications. These uploads should be disabled whilst you are working.

24.19 Any paper files or documents taken from the office to work at home must be protected in transit and in your home. Ideally transported in a secure form such as a briefcase or encrypted memory stick and never left unattended in a vehicle.

24.20 Keep paperwork secure at home and out of sight of members of your family, visitors to the premises and others.

Loss or Theft

24.21 In the event that a device, whether personal or Company owned, is lost, stolen or its security is compromised, you MUST immediately, or if out of hours within an hour of the business reopening the next working day, report this to the **Data Protection Manager**, in order for them to assist in changing passwords to all company services, considering the extent of the loss and reporting as a data breach if appropriate.

24.22 You must also cooperate with the management team in wiping the device remotely where possible and necessary, even if such a wipe results in the loss of your own data, such as photos, contacts etc.

24.23 The Company will not normally monitor the content of your personal devices. However, the Company reserves the right to monitor and log data traffic transferred between your device and company systems, both over internal networks and via the Internet.

24.24 In exceptional circumstances, for instance where the Company requires access in order to comply with its legal obligations or requirements from a lawful authority such as the Information commissioner or the Police. The Company will require access to company data and information stored on a personal device. Under these circumstances, all reasonable efforts are made to ensure that there is no access to an employee's private information.

Approval for Working remotely

24.25 Home and/or Remote working must not begin until authorised by the Company.

24.26 Applications to begin Home/Remote working should be made in writing to your line manager who will consider requests for home working in consultation with Human Resources.

©TransitionLaw2025

25 Generative AI Policy

25.1 The Company recognises the potential of artificial intelligence (AI) to transform the way we work, improve the services we provide and our competitiveness.

25.2 We are committed to ensuring we use AI tools in a secure and responsible way, respecting confidentiality and third party rights. This includes any AI tools used by third parties on our behalf.

25.3 This policy provides guidance to staff on using and deploying generative AI tools in the course of your work, the circumstances in which we will monitor use of generative AI, and the action we will take if this policy is breached. It should be read in conjunction with other policies that are relevant to the use of AI in the workplace, eg:

25.3.1 data protection policy

25.3.2 information security policy

25.3.3 Internet Email and Communications policy

25.4 This policy applies to all individuals, including employees, workers, temporary and agency workers, contractors, interns, volunteers and apprentices (referred to as 'staff' in this policy).

25.5 We will review and update this AI policy regularly to take account of changes in technology, legal obligations and best practice. We will circulate any new or modified policy to staff when it is adopted.

25.6 The Data Protection Manager is responsible for monitoring and implementing this policy. If you have any questions or comments on this policy, please contact the Data Protection Manager.

What is meant by generative AI?

25.7 There is no single definition of artificial intelligence (AI). Broadly speaking it is the simulation of human intelligence in machines, generally computer systems.

25.8 AI tools can learn, problem-solve, make decisions, and understand language. This can be contrasted with non-AI pre-programmed tools, which generally apply the same set of rules each time unless a human intervenes to update the rules. An AI tool can learn and adapt without human intervention.

25.9 There are several types of AI, including generative, predictive and extractive:

Generative AI	An AI tool that *generates* new, realistic content in the form of text, audio, computer code, data or images etc For example, using an AI tool to: —generate a marketing blog post —improve an email you have already written —write a product description or a job description

©TransitionLaw2025

	—write a script or slides for a presentation —check, amend and improve your grammar, spelling and writing style —summarise a report or large block of text —power sophisticated chatbots, or —write software code or find common bugs in code
Predictive AI	An AI tool that analyses data to make *predictions*, eg about: —customers' buying behaviour, or —how busy the office will be at any particular time
Extractive AI	An AI tool that *extracts* data from the dataset it has been trained on (but can't create data)

25.10 This policy focuses on generative AI but it also applies more broadly to all forms of AI used for business purposes. *eg ChatGPT and Microsoft Copilot* are examples of generative AI providers.

AI guiding principles

25.11 Our responsible AI approach means that we:

25.11.1 consider the real-world impact of any AI that we may use or develop;

25.11.2 take action to avoid the creation or reinforcement of bias;

25.11.3 can explain how the AI we use works;

25.11.4 create accountability through audit, governance and human oversight; and

25.11.5 respect privacy and champion robust data governance.

Potential benefits of using AI in the workplace

25.12 Generative AI can be an efficient tool for producing text, images or code quickly and to a specification.

25.13 Generative AI provides opportunities for efficiencies, eg *when used in brainstorming ideas or creating a first draft.*

25.14 AI has the potential to improve productivity, personalise the customer experience and accelerate product/service developments. It may be capable of completing repetitive, manual high-volume tasks, freeing up our staff for more interesting value-added work.

©TransitionLaw2025

Potential risks of using generative AI in the workplace

25.15 To understand the potential risks of using AI in the workplace it is helpful to understand how generative AI tools are trained and how they work.

25.16 Generative AI tools are trained on colossal banks of existing content from various sources, called datasets. They learn to identify patterns in those datasets. The more advanced generative AI tools are able to identify those patterns without human intervention or supervision. Some generative AI tools will then use additional input or prompt data and feedback from users to continue to self-train (a prompt is a question or request you write for the AI tool to answer or solve).Text-generating AI tools often work by selecting the most-likely next word in a sentence and the one after that (to create text), whereas image-generating AI tools often work by selecting the next pixel.

25.17 This raises several questions including:

25.17.1 can the generative AI tool reuse, recycle or republish information we input—and make that information available for other users, directly or indirectly?

25.17.2 do we have the right or permission to put information that belongs to someone else into the AI tool, eg confidential information, personal data or copyright material belonging to someone else?

25.17.3 who owns the intellectual property (eg the copyright) in the text (or image/code) produced by the AI tool?

25.17.4 can we rely on the accuracy of the text or results generated by the AI tool?

25.17.5 are there any other risks, eg biases in the data that the AI tool was trained on that might cause it to discriminate?

25.18 Some of these AI risks are overlapping and the following sections expand on the main themes.

Privacy and confidentiality risks

25.18.1 Generative AI tools can exacerbate data and privacy risks.

25.18.2 Data protection law requires that we must have a lawful ground for collecting and using personal data. However, the lawful ground on which we originally collected personal data may not cover us for using that data in a generative AI tool. Unless additional consent is obtained, entering that personal data into a publicly-accessible generative AI tool (which can store the information indefinitely, recycle and reuse it) is likely to constitute a data protection breach.

25.18.3 Likewise, using publicly-accessible generative AI tools runs the risk of exposing company-owned (proprietary) information.

Intellectual property (IP) and trade secrets

25.18.4 AI tools can increase the risk that our IP and trade secrets will be improperly disclosed. Most publicly-accessible AI tools don’t guarantee the information you input into the tool will not be used to train the AI model. This means our IP could be reproduced or made available to other users in some form.

©TransitionLaw2025

25.18.5 AI-generated content may also infringe IP owned by third parties, particularly copyrights. This is effectively the same risk as above, but in reverse, ie we put third party information into an AI tool without proper licence, thereby breaching the third party's IP. This could be information belonging to a customer, supplier or party completely unconnected to our business.

25.18.6 There is also an indirect risk where our IP is shared with third-party suppliers, eg marketing agents. While we must take care to avoid inputting our valuable IP into an AI tool, we must also ensure that our third-party providers do not do exactly that with our IP, eg to produce marketing collateral.

Accuracy

25.19 Where generative AI does not have the information to provide the information you have requested, it may still attempt to provide you with an output. It could do this by simply making things up (or 'hallucinating').

25.19.1 Relying on a response or text produced from an AI tool without checking could have a range of negative outcomes including damage to our reputation.

25.19.2 As well as the risk of hallucinations, the output of an AI tool may not be guaranteed to be 100% accurate. Generally speaking, accuracy in AI refers to how often the AI system guesses the correct answer, measured against correctly labelled test data. This is known as statistical accuracy.

25.19.3 In many cases, the outputs of an AI system are not intended to be treated as factual information, eg about an individual, but rather a statistically informed guess as to something which may be true about the individual now or in the future. Where this is the case, it is important that we do not misinterpret the AI as being factually or statistically accurate.

Bias

25.19.4 Another concern with generative AI (and other forms of AI) is the potential for bias to be embedded within the AI tool. This bias can then be perpetuated as the AI tool operates and develops, inadvertently leading to the creation of discriminatory content or decisions. This is not necessarily deliberate, the AI tool may simply be reflecting the unconscious bias of its creators or other users.

25.19.5 There are two main potential sources of bias—the data itself and the algorithm applied to the data by the AI tool:

(a) if the data used to train a generative AI tool is biased (eg towards a particular race or gender), the AI tool is likely to produce biased content; whereas

(b) if bias is embedded into the AI algorithm (the coded instructions that tells the AI tool how to function), the output is likely to be biased even if the data itself is not biased.

©TransitionLaw2025

Who may use generative AI for work purposes and when?

25.20 Access to internal and publicly-accessible AI tools, platforms or related systems is restricted to authorised staff only..

25.21 You must not download and/or use third party add-ins without approval from your line manager.

Guidelines for staff on using generative AI tools and platforms

25.22 If you wish to use another generative AI tool, you should contact the Data Protection Manager to ask whether you can be given authority to use it.

25.23 You must not share your access credentials or allow others to use generative AI tools on your behalf.

25.24 You must not use generative AI in any way that could be considered discriminatory, or could give rise to defamation, harassment, intimidation or bullying or in any way that could harm the reputation of another.

25.25 You must not use generative AI to create illegal content or for illegal purposes.

25.26 You must not use offensive, obscene or abusive language, graphics or imagery when inputting content into generative AI and must not attempt to create content which is offensive, obscene or abusive through your use of generative AI tools.

25.27 Unless specifically authorised to do so, you must not input into a publicly-accessible generative AI tool:

25.27.1 the company's trademarks, brands, logos or any other identifying material;

25.27.2 the company's name, email or other contact details (other than where required to input your work email address);

25.27.3 proprietary company information;

25.27.4 customer or supplier materials, information or data;

25.27.5 trade secrets, confidential or valuable information;

25.27.6 usernames, passwords (other than for the AI tool itself), and security tokens; or

25.27.7 personal data, ie information or data from which any living individual can be identified—including personal data relating to employees, customers, suppliers and unconnected third parties.

This includes inputting data as training data to a generative AI technology or in any instruction or prompt (a question or request that you write for the generative AI tool to answer or solve).

25.28 When using generative AI in the workplace, you must always use your company email address to create and log in to any generative AI account (do not use your personal email address or login credentials).

©TransitionLaw2025

25.29 You must not in any way provide or suggest any endorsement or recommendation by the company of any third party generative AI technology.

25.30 You must protect your login credentials and ensure any generative AI accounts that you hold are not accessible to unauthorised third parties. The use of multi-factor authentication is advised in respect of any generative AI tools and technologies used.

25.31 Your use of generative AI in the workplace must be limited to business-related purposes and should, at all times, be in accordance with all applicable laws (including data protection and privacy laws).

25.32 You are responsible for ensuring the generated content aligns with our values, ethics and quality standards. Before using any AI generated content, you must carefully review it and ensure you do not use content that:

25.32.1 discloses confidential or proprietary company information without approval from your line manager;

25.32.2 reveals personal data about any individual, without approval from your line manager;

25.32.3 has the potential to breach the intellectual property rights of a third-party;

25.32.4 is misleading and/or cannot be verified;

25.32.5 is discriminatory, otherwise biased or offensive.

25.33 You must comply with the terms and conditions of the generative AI technology that you use, unless such terms and conditions are in conflict with or contradict our policies or your terms of employment, in which case you should seek advice from your line manager.

Personal use of generative AI

25.34 You may make reasonable use of generative AI tools for personal use using the company's computers, networks and/or systems (including via smartphones or tablets), provided use is minimal and takes place substantially out of normal working hours (ie during your lunch break or before or after work), it does not interfere with your duties and business and office commitments and is strictly in accordance with this policy.

25.35 Any unauthorised use of generative AI is strictly prohibited. Permission to use the company's systems to access generative AI tools for personal use may be withdrawn at any time at the company's discretion.

Monitoring

25.36 Our internet, email and communications policy applies to the use of generative AI technologies via the company's systems or network, in particular in relation to the company's right to monitor, intercept and read communications.

25.37 We will also monitor how our supplier's and customers use generative AI generally and any use of company information or information concerning the company by them or by our competitors.

©TransitionLaw2025

Responsibility for compliance

25.38 All employees are responsible for ensuring their own use of generative AI is in accordance with this policy, and must, in particular, make themselves aware of, and comply with, their responsibilities, as outlined in this policy, to protect confidential and sensitive information when using generative AI.

25.39 Managers and supervisors are responsible for ensuring their teams are aware of and comply with this policy and they must report any breach of this policy to the Data Protection Manager.

25.40 The Data Protection Manager is responsible for handling any complaints concerning violation of or non-compliance with this policy, including any allegations of harassment, discrimination, or bias that may be raised by employees, customers, suppliers or other third parties.

Breaches of this policy

25.41 Because of the importance of this policy, failure to comply with any requirement of it may lead to disciplinary action and this action may lead to dismissal for gross misconduct. If you are not an employee, breach of this policy may result in termination of your contract with immediate effect.

25.42 You should note in particular that inputting company materials, data or information, including commercially sensitive or confidential information, to generative AI tools may amount to misconduct even if it takes place:

25.42.1 on a personal account with appropriate privacy settings;

25.42.2 outside normal working hours; and/or

25.42.3 without using the company's computers, systems and networks.

25.43 If, in the course of your employment, you become aware of any misconduct or wrongdoing by any employee, officer, worker or agent of the company in breach of this or related policies, you must report it to your line manager.

25.44 You must also make a report to your line manager if you become aware that:

25.44.1 a customer or supplier has input confidential or proprietary company information or personal data relating to any of our staff into a publicly-accessible AI tool; or

25.44.2 a publicly-accessible AI tool has otherwise produced output that includes confidential or proprietary company information or personal data relating to any of our staff;

25.44.3 we may have used an AI tool in a way that infringes IP owned by third parties or infringes the data protection rights of a third-party, whether deliberately or inadvertently.

25.45 Staff who feel that they have been harassed, bullied or defamed because of material created or generated through the use of generative AI by a colleague should inform their line manager.

©TransitionLaw2025

26 Internet, Email and Communications Policy

26.1 The Company recognises that the use of email and the internet can save time and expense, and is an important part of the way we work. However, it brings with it certain risks, some of which may involve potential legal and financial liabilities for both the Company and the individual, eg:

26.1.1 inadvertently entering into contracts or commitments on behalf of the Company;

26.1.2 introducing viruses into the Company's systems;

26.1.3 breaching copyright or licensing rights;

26.1.4 breaching data protection rights;

26.1.5 breaching confidentiality and security;

26.1.6 defamation; and/or

26.1.7 bullying, harassment and discriminatory conduct.

26.2 This policy aims to guard against those risks. It is therefore important that all staff read the policy carefully and ensure that they use the internet, email and other communication systems in accordance with it. If you are unsure whether something you are about to do complies with this policy, you should seek advice from your line manager.

26.3 This policy also explains when we will monitor the use of email and the internet and the action we will take if the terms of this policy are breached.

26.4 References in this policy to 'email' apply equally to other electronic communications, messaging tools and posts.

Scope

26.5 This policy applies:

26.5.1 to all staff, including employees, workers, temporary and agency workers, interns, volunteers and apprentices, and to consultants and other contractors who have access to our computer and other communications systems;

26.5.2 to personal use of our systems and equipment in any way that reasonably allows others to identify any individual as associated with the Company;

26.5.3 to the use of our email, telephone and internet systems both in the workplace and from outside it, eg via remote access, and to the use of a Company laptop, tablet, mobile phone, smartphone or personal digital assistant (PDA).

26.6 You must familiarise yourself with this policy and comply with its terms.

26.7 You should also refer to our data protection policy and data protection privacy notice and, where appropriate, to our other relevant policies including in relation to generative AI.

©TransitionLaw2025

Use of the Company's computer systems

26.8 You may use our computer systems (including equipment) for authorised purposes only. If you wish to use the Company's systems or equipment for another purpose, you must obtain express permission from your line manager before doing so.

26.9 To reduce the risk to the Company's systems or network of virus infections, hacking and other unauthorised access attempts, you may only access the Company's systems and network as follows:

26.9.1 from your workplace or other Company premises, using authorised equipment only;

26.9.2 remotely (via broadband, dial up, etc, using authorised equipment via secure means, eg VPN software only; or

26.9.3 remotely, using unauthorised equipment, eg your home computer or an internet café terminal, providing sufficient security arrangements are in place to protect your activity.

26.10 You must not use any software owned or licensed by the Company for any purpose other than those of our business without express permission from your line manager or as otherwise permitted by the terms of this policy, and you must not copy, download or install any software without first obtaining express permission from your line manager.

Email use—general

26.11 All communications, including email, should reflect the highest professional standards at all times. In particular, you must:

26.11.1 keep messages brief and to the point;

26.11.2 check emails carefully before sending, including spelling and grammar;

26.11.3 ensure that all emails sent from the Company include the current disclaimer wording;

26.11.4 ensure that an appropriate heading is inserted in the subject field; and

26.11.5 check the recipient(s) before pressing the send button—not only can it be embarrassing if a message is sent to the wrong person, it can also result in the unintentional disclosure of confidential information about the Company, a client/customer or other third parties.

26.12 You must not send messages from another person's email address (unless authorised in the proper performance of their duties), or under an assumed name.

26.13 You must not send or post messages or material that are offensive, obscene, defamatory or otherwise inappropriate in the work environment.

26.14 You must not send or post any message or material which could be regarded by the recipient or any other person as personal, potentially offensive or frivolous.

26.15 You should not send or post anything in an email that they would not be comfortable writing (or someone else reading) in a letter. Emails leave a retrievable record and, even when deleted, can be recovered from our back-up system or an individual's computer. They are

©TransitionLaw2025

admissible as evidence in legal proceedings and have been used successfully in libel and discrimination cases, and they can also be reviewed by regulators.

26.16 You must not create congestion on the Company's systems or network by sending trivial messages, by unnecessary copying or forwarding of messages to recipients who do not need to receive them, or by sending or forwarding chain mail, junk mail, cartoons, jokes or gossip.

26.17 You must use a Company email address for sending and receiving work-related emails and must not use your own personal email accounts to send or receive emails for the purposes of our business. You must not send (inside or outside work) any message in our name unless it is for an authorised, work-related purpose.

26.18 You must not send unsolicited commercial emails to anyone with whom you do not have a prior relationship without the express permission of the relevant manager.

26.19 You must be vigilant when using our email system. Computer viruses are often sent by email and can cause significant damage to the Company's information systems or network. Be particularly cautious in relation to unsolicited emails from unknown sources.

26.20 If you suspect that an email may contain a virus, you should not reply to it, open any attachments to it or click on any links in it and must contact your line manager immediately for advice.

Emails—confidentiality

26.21 Do not assume that emails sent or received internally or externally are private and confidential, even if marked as such. Email is not a secure means of communication and third parties may be able to access or alter messages that have been sent or received. Do not send any information in an email which you would not be happy being publicly available. Matters of a sensitive or personal nature should not be transmitted by email unless absolutely unavoidable and if so, should be clearly marked in the message header as highly confidential.

26.22 Lists of contacts compiled by you during the course of your employment and stored on our email application, information manager and/or other database(s) (irrespective of how they are accessed) belong to us. You must not copy or remove such lists for use outside your employment or after your employment ends.

Emails—personal use

26.23 Although the email system is primarily for business use, we understand that you may occasionally need to send or receive personal emails while at work.

26.24 The sending of personal emails using the work email address is therefore permitted. When sending personal emails using the work email address, you should show the same care as when sending work-related emails.

26.25 Reasonable personal use of our systems or network to send personal email is also permitted, provided that it does not interfere with the performance of any individual's duties and the terms of this policy are strictly adhered to. We reserve the right, at our absolute discretion, to withdraw this privilege at any time and/or to restrict access for personal use.

26.26 Personal use must meet these conditions (in addition to those set out elsewhere in this policy):

©TransitionLaw2025

26.26.1 it must be minimal (both in terms of time spent and frequency) and reasonable and must take place mainly outside normal working hours, ie during lunch or other breaks, or before and after work;

26.26.2 personal emails must be labelled ‘Personal’ in the subject header and in the sensitivity settings;

26.26.3 personal use must not affect the job performance of you or your colleagues, or otherwise interfere with our business; and

26.26.4 it must not commit us to any marginal costs.

Emails—monitoring

26.27 We may monitor the email and instant messaging systems or network in the workplace for the following reasons:

26.27.1 to determine whether they are communications relevant to the carrying on of our business;

26.27.2 if you are absent from work, to check communications for business calls to ensure the smooth running of the business;

26.27.3 to record transactions;

26.27.4 where we suspect that messages being sent or received are:

(a) detrimental to the Company;

(b) in breach of an individual’s contract, or this policy;

(c) in breach of data protection rights;

26.27.5 to monitor staff conduct;

26.27.6 to investigate complaints, grievances or criminal offences.

26.28 When monitoring incoming or outgoing emails, we will, unless exceptional circumstances apply:

26.28.1 look at the sender or recipient of the email and the subject heading only; and

26.28.2 avoid opening emails marked ‘Private’ or ‘Personal’.

26.29 We do not as a matter of policy routinely monitor employees' use of the internet or the content of email messages sent or received. However, we have a right to protect the security of our systems or network, check that use of the system is legitimate, investigate suspected wrongful acts and otherwise comply with legal obligations imposed upon us. To achieve these objectives, we may carry out random spot checks on the system which may include accessing individual email messages or checking on specific internet sites searched for and/or accessed by individuals.

26.30 We will only intercept (ie open) outgoing or incoming emails, received emails, sent emails and draft emails where relevant to the carrying on of our business and where necessary:

©TransitionLaw2025

26.30.1 to determine whether the message is relevant to the carrying on of our business;

26.30.2 to establish the existence of facts;

26.30.3 to check whether regulatory or self-regulatory practices or procedures to which we or our staff are subject have been complied with, ie to detect unauthorised use of the system;

26.30.4 to check whether staff using the system in the course of their duties are achieving the standards required of them;

26.30.5 for the purpose of investigating or detecting the unauthorised use of the system;

26.30.6 for the purpose of preventing or detecting crime; or

26.30.7 for the effective operation of the telecommunication system.

Telephones—personal use

26.31 Although the telephone system is primarily for business use, we understand that you may occasionally need to make or receive personal telephone calls while at work. The making or receiving of personal telephone calls while at work using our telephone system AND/OR your personal mobile phone is therefore permitted.

26.32 Personal use must meet these conditions (in addition to those set out elsewhere in this policy):

26.32.1 it must be minimal (both in terms of time spent and frequency) and reasonable and must take place mainly outside normal working hours, ie during lunch or other breaks, or before and after work;

26.32.2 it must not affect the job performance any member of staff or otherwise interfere with our business;

26.32.3 it must not commit us to any marginal costs; and

26.32.4 you may not use the telephone during working hours to perform work for yourself or another employer, or to look for work;

26.33 Our telephone system may not be used for premium rate or international calls.

Telephones—monitoring

26.34 We may monitor the use of our telephone system, and Company mobile phones (including smartphones) for the following reasons:

26.34.1 if you are absent from work, to check communications (including your voicemail) for business calls to ensure the smooth running of the business;

26.34.2 to record transactions;

26.34.3 where we suspect that an individual is acting in a way that is:

(a) detrimental to the Company;

©TransitionLaw2025

(b) in breach of the individual's contract, or this Policy;

(c) in breach of data protection rights;

26.34.4 to monitor staff conduct;

26.34.5 to investigate complaints, grievances or criminal offences.

26.35 When monitoring telephones, we will, unless exceptional circumstances apply, look at the numbers from which calls are received and the numbers dialled and the duration and frequency of calls.

26.36 We will only intercept (ie listen to) telephone calls or saved messages where relevant to the carrying on of our business and where necessary:

26.36.1 to determine whether the message is in fact relevant to the carrying on of our business;

26.36.2 to establish the existence of facts;

26.36.3 to check whether regulatory or self-regulatory practices or procedures to which we or our staff are subject have been complied with, ie to detect unauthorised use of the system;

26.36.4 to check whether staff using the system in the course of their duties are achieving the standards required of them;

26.36.5 for the purpose of investigating or detecting the unauthorised use of the system;

26.36.6 for the purpose of preventing or detecting crime; or

26.36.7 for the effective operation of the telecommunication system.

Internet—general

26.37 Access to the internet during working time is primarily for matters relating to your work duties and employment. Reasonable, limited personal use of the internet is permitted.

26.38 Any unauthorised use of the internet is strictly prohibited. Unauthorised use includes (but is not limited to):

26.38.1 creating, viewing or accessing any webpage, or posting, transmitting or downloading any image, file or other information that is unrelated to your employment and, in particular, which could be regarded as pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to us or to our clients/customers and/or suppliers;

26.38.2 engaging in computer hacking and/or other related activities; and

26.38.3 attempting to disable or compromise security of information contained on our systems or network or those of a third party.

26.39 Staff are reminded that such activity may also constitute a criminal offence.

26.40 Posts placed on the internet may display our address. For this reason you should make certain before posting information that the information reflects our standards and policies.

©TransitionLaw2025

Under no circumstances should information of a confidential or sensitive nature be placed on the internet. You must not use the Company's name in any internet posting (inside or outside work) unless it is for a work-related purpose.

26.41 Information posted or viewed on the internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the internet may be done only by express permission from the copyright holder. You must not act in such a way as to breach copyright or the licensing conditions of any internet site or computer program.

26.42 We may block or restrict access to any website at its discretion.

Internet—personal use

26.43 Reasonable personal use of our systems or network to browse the internet is allowed provided that it does not interfere with the performance of your duties and the terms of this policy are strictly adhered to. We reserve the right, at its absolute discretion, to withdraw this privilege at any time and/or to restrict access for personal use.

26.44 Personal use must meet these conditions (in addition to those set out elsewhere in this policy):

26.44.1 it must be minimal (both in terms of time spent and frequency) and reasonable and should take place mainly outside normal working hours, ie during lunch or other breaks, or before and after work;

26.44.2 it must not affect the job performance of any member of staff or otherwise interfere with our business; and

26.44.3 it must not commit the Company to any marginal costs.

Internet—monitoring

26.45 We may monitor internet usage (including searches made, the IP addresses of sites visited, and the duration and frequency of visits) if we suspect that an individual has been using the internet in breach of the contract of employment or this policy, eg:

26.45.1 by viewing material that is pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to us or to our clients/customers;

26.45.2 by spending an excessive amount of time viewing websites that are not work-related.

26.46 Monitoring may include internet usage at the workplace, internet usage outside the workplace during working hours using Company systems or network and internet usage using hand-held or portable electronic devices.

Passwords and security

26.47 You are personally responsible for the security of all equipment allocated to or used by you. You must not allow equipment allocated to you to be used by any other person, other than in accordance with this policy.

26.48 You must use passwords on all IT equipment allocated to you, and keep any password allocated to you confidential and change your password regularly.

©TransitionLaw2025

26.49 You must not use another person's username and/or password to access our systems or network, nor allow any other person to use your password(s). If it is anticipated that someone may need access to your confidential files in your absence, you should arrange for the files to be copied to a network location that is properly secure where the other person can access them or give the person temporary access to the relevant personal folders.

26.50 You must log out of the system or lock your computer when leaving your desk for any period of time. You must log out and shut down your computer at the end of the working day.

Company systems and data security

26.51 You must not download or install software from external sources without prior authorisation from your line manager.

26.52 You must not connect any personal computer, mobile phone, laptop, tablet, USB storage device or other device to our systems or network without express prior permission from your line manager. Any permitted equipment must have up-to-date anti-virus software installed on it and we may inspect such equipment in order to verify this.

26.53 You must not run any '.exe' files, particularly those received via email, unless authorised to do so in advance. Unauthorised files should be deleted immediately upon receipt without being opened.

26.54 You must not access or attempt to access any password-protected or restricted parts of our systems for which you are not an authorised user.

26.55 You must inform your line manager immediately if you suspect your computer may have a virus and must not use the computer again until informed it is safe to do so.

26.56 All laptop, tablet, smartphone and mobile phone users should be aware of the additional security risks associated with these items of equipment. All such equipment must be locked away in a secure location if left unattended overnight.

27 Social Media Policy

27.1 The Company recognises that internet and social media platforms are used as a means of communication both at work and at home. This policy outlines the standards we require staff to observe when using social media, the circumstances in which we will monitor your use of social media and the action we will take if this policy is breached. This policy should be read in conjunction with our Internet, email and communications policy, which sets out how the Company's internet and email systems and networks can be used by our staff and representatives.

27.2 This policy applies to all individuals, including employees, workers, temporary and agency workers, contractors, interns, volunteers and apprentices (referred to as 'staff' in this policy).

27.3 Staff should refer to the Company's data protection privacy notice and, where appropriate, to its other relevant policies.

Social media

27.4 In this policy, 'social media' means internet-based applications which allow users to collaborate or interact socially by creating and exchanging content, such as social networks or platforms, community sites, blogs, microblogging sites, wikis, web forums, social bookmarking

©TransitionLaw2025

services and user rating services. Examples include Facebook, LinkedIn, YouTube, Instagram, X, Bluesky, Tumblr, TikTok, Flickr, SlideShare, Foursquare and Pinterest and the review areas of e-commerce sites.

27.5 Social media platforms allow us to build connections and to share ideas and content more broadly and quickly, and we support their use. However, improper use of social media may give rise to a breach of your contract and/or our policies, and/or defamation (ie damaging the good reputation of another person or organisation), breach of data protection laws, misuse of our confidential information or that of our customers, clients and/or suppliers and/or reputational damage.

27.6 This policy does not seek to regulate how staff use social media in a purely private capacity, provided that use has no bearing on the Company or its activities. This policy is intended to ensure that staff understand the rules governing their use of social media in relation to their work for us, or when referencing the Company, or where use of social media may affect us or our activities. It is designed to help you use these platforms and services responsibly, so as to minimise the risks set out above and to ensure consistent standards of use of social media. This policy therefore applies where:

27.6.1 your use of social media relates to the Company or its activities;

27.6.2 your use of social media relates to, or is otherwise connected with, your work, whether the intended use is personal or professional; and/or

27.6.3 you represent yourself, or are otherwise identifiable, as someone employed by, or otherwise associated with, the Company.

27.7 This policy applies to your use of social media whether on a Company, personal or other device.

General rules for use of social media

27.8 You must not use your work email address to sign up for personal use of social media platforms.

27.9 You should have no expectation of privacy or confidentiality in anything you create or share on social media platforms. When you create or exchange content using social media you are making a public statement. As such, your content will not be private and can be reposted, copied or forwarded to third parties without your consent. You should therefore consider the potential sensitivity of disclosing information (such as health information) on a platform. Once sensitive or confidential information (or offensive or defamatory information) has been disclosed, it cannot be recovered and this may result in liability both for the Company and also for you personally.

27.10 Bear in mind that, even if you are using social media in a personal capacity, other users who are aware of your association with us might reasonably think that you speak on our behalf. You should always take account of any adverse impact your content might have on our reputation or our relationships with clients, customers, suppliers and other business partners.

27.11 When creating or exchanging content on a social media platform, you must at all times comply with your contract of employment (or other contractual arrangements) with us, our disciplinary rules and any of our policies that may be relevant. In particular you must:

©TransitionLaw2025

27.11.1 not harass, sexually harass or bully other members of staff, or customers, clients, suppliers or other third parties;

27.11.2 not discriminate against other members of staff or third parties;

27.11.3 not breach our data protection or Internet, email and communications policies;

27.11.4 respect any confidentiality obligations owed by you or us, and not disclose commercially sensitive material or infringe any intellectual property or privacy rights of the Company or any third party;

27.11.5 not make defamatory or disparaging statements about the Company, its shareholders, employees, customers, clients, suppliers or competitors;

27.11.6 not create or exchange or link to abusive, obscene, discriminatory, derogatory, defamatory or pornographic content;

27.11.7 not upload, post or forward any content belonging to a third party unless you have that third party's consent;

27.11.8 ensure that any quotes from third party material are accurate;

27.11.9 check that a third party website permits you to link to it before including a link and ensure that the link makes clear to the user that the link will take them to the third party's site; and not post, upload, forward or post a link to chain mail, junk mail, cartoons, jokes or gossip.

27.12 You should be honest and open but also be mindful of the impact your posting on a social network or platform may have on the perception of the Company.

27.13 If you make a mistake in a posting, be prompt in admitting and correcting it.

27.14 Do not escalate 'heated' discussions. Try to be conciliatory and respectful and quote facts to lower the temperature and correct misrepresentations. Never contribute to a discussion if you are angry or upset; return to it later when you can contribute in a calm and rational manner.

27.15 Avoid posting in relation to or discussing topics that may be inflammatory, such as politics or religion.

27.16 You should regularly review the privacy settings on your personal social media accounts and appropriately restrict the people who can read your comments. Review the content of your personal social media accounts on a regular basis and delete anything that could reflect negatively on you in a professional capacity or on the Company.

Using work-related social media

27.17 We recognise the importance of the internet and social media in shaping public thinking about the Company, our services, staff, clients, customers and other business partners. We also acknowledge that our staff can have an important role to play in shaping industry/sector conversation and direction through interaction in social media.

27.18 Our staff are therefore permitted to interact on approved social media platforms about industry/sector developments.

©TransitionLaw2025

27.19 When undertaking permitted work-related social media interaction, in addition to the general rules above, you must:

27.19.1 clearly identify yourself, including your name and job title, and use the following disclaimer: '*The views expressed are my own and do not necessarily reflect the views of my employer*';

27.19.2 ensure that all communications are of high quality (in terms of content and form) including being grammatically correct, accurate, objectively justifiable, reasonable and appropriate for the intended audience;

27.19.3 not provide references or recommendations for anyone else on social media (whether employment or business recommendations) in any way that suggests any endorsement or recommendation by the Company. If you wish to provide a reference or recommendation, you should seek advice from your line manager and ensure that any such reference or recommendation can be withdrawn at any time as we may require;

27.19.4 if you become aware of adverse criticism of the Company or of content you have created or shared, inform your line manager. Do not respond without their express approval;

27.19.5 comply with the terms and conditions and policies of the social media platforms you use;

27.19.6 maintain good information security practices. Use strong passwords and make appropriate use of security and privacy settings on social media platforms, and follow our email, internet and communications and information security policies, guidelines and standards;

27.19.7 seek approval from your line manager before creating or exchanging comments on colleagues, customers, clients, suppliers or competitors;

27.19.8 before you begin communication on a social media platform, evaluate your audience by gaining an insight into the type of content that is published and note any unwritten rules that are followed in discussions;

27.19.9 not use our trade marks, brands or logos or other identifying material

Personal use of social media platforms

27.20 You may make reasonable use of social media platforms for personal use outside working hours using our computers, networks and/or systems (including via smartphones or tablets), provided use is minimal and takes place substantially out of normal working hours (ie during your lunch break or before or after work), it does not interfere with your duties and business and office commitments and is strictly in accordance with this policy.

27.21 Any unauthorised use of social media platforms is strictly prohibited. Permission to use our systems to access social media platforms for personal use may be withdrawn at any time at our discretion.

©TransitionLaw2025

Monitoring

27.22 Our internet, email and communications policy, in particular in relation to our right to monitor, intercept and read communications, applies equally to use of social media platforms via the Company's systems or network.

27.23 We will also monitor how we use social media generally and what is said about us and about our competitors.

27.24 We may monitor your LinkedIn and other business-related social media profiles during your notice period and during the period of any relevant post-termination restrictions to which you are subject, for the purposes of our legitimate interests, ie to ensure that any non-competition provision is complied with. We will only carry out such monitoring where there are no other, less invasive, means available.

Breaches of this policy

27.25 Staff are also reminded that, in certain circumstances, an act that breaches this policy may also constitute a criminal offence.

27.26 If, in the course of using social media, you become aware of any misconduct or wrongdoing by any employee, officer, worker or agent of the Company, you must report it to your line manager.

27.27 You may be required to remove content created or shared by you which we deem to be in breach of this policy.

27.28 Employees who feel that they have been harassed or bullied because of material posted or uploaded by a colleague onto a social media platform should inform their line manager.

©TransitionLaw2025

Business Compliance Document

PART FOUR of FIVE

DATA RIGHTS & BREACH POLICIES

©TransitionLaw2025

28 Data Subject Access Requests

28.1 The Company holds personal data (or information) about job applicants, employees, clients, customers, suppliers, business contacts and other individuals for a variety of business purposes.

28.2 The individuals (known as 'data subjects') have a general right to find out whether we hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request. The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that we are undertaking.

28.3 The **Data Protection Manager** is responsible for ensuring:

28.3.1 that all data subject access requests are dealt with in accordance with UK GDPR and other relevant legislation and guidance; and

28.3.2 that all staff have an understanding of UK GDPR and other relevant legislation and guidance in relation to data subject access requests and their personal responsibilities in complying with the relevant aspects of UK GDPR and other relevant legislation and guidance.

28.4 This policy provides guidance on handling data subject access requests and is intended for internal use. It is not a privacy policy or statement, and is not to be made routinely available to third parties.

28.5 This policy provides guidance on:

28.5.1 what to do if you receive a data subject access request; and

28.5.2 how to decide whether a request for information is a data subject access request.

28.6 Failure to comply with the right of access under UK GDPR puts both staff and the Company at a potentially significant risk. The Company takes compliance with this policy very seriously.

28.7 We will review and update this policy annually in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

28.8 If you have any questions regarding this policy, please contact the **Data Protection Manager**.

How to recognise a data subject access request (DSAR)

28.9 A data subject access request is a request from an individual or from someone acting with their authority, e.g. a relative or solicitor for the information the individual is entitled to ask for under UK GDPR, namely:

28.9.1 for confirmation as to whether we process personal data about the individual and, if so:

28.9.2 for access to that personal data

28.9.3 and certain other supplementary information

©TransitionLaw2025

28.10 Such a request will typically be made in writing but may be made orally (e.g. during a telephone conversation). The request may refer to 'UK GDPR', 'GDPR' and/or to 'data protection' and/or to 'personal data' **but does not need to do so** in order to be a valid request. For example, a letter which states 'please provide me with a copy of all the information that you have about me' will be a data subject access request and should be treated as such.

28.11 All data subject access requests should be immediately directed to the **Data Protection Manager** for immediate attention.

What to do when you receive a data subject access request

28.12 If you receive a data subject access request, you must immediately take the steps to alert the **Data Protection Manager**.

28.13 There are limited timescales within which we must respond to a request and any delay could result in our failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

28.14 The timescales referred to in this policy must be calculated from the day we receive a request (whether it is a working day or not) until the corresponding calendar date in the next month, for example if a request is received on 1 September, the information must be provided by 1 October.

28.15 If you are in any way unsure as to whether a request for information is a data subject access request, please contact the **Data Protection Manager**.

28.16 If you receive a data subject access request by email, you must immediately forward the request to the **Data Protection Manager**.

28.17 If you receive a data subject access request orally, you must:

28.17.1 take the name and contact details of the individual;

28.17.2 inform the individual orally that you will notify the **Data Protection Manager** that the individual has made an oral request and say the **Data Protection Manager** will contact them in relation to the request;

28.17.3 immediately inform the **Data Protection Manager** and provide the individual's contact details and details of the oral request and the date on which it was received.

28.18 You will receive confirmation when the request has been received by the **Data Protection Manager**. If you do not receive such confirmation within **two** working days of sending it, you should contact the **Data Protection Manager** to confirm safe receipt.

28.19 You must not take any other action in relation to the data subject access request unless the **Data Protection Manager** has authorised you to do so in advance and in writing.

Advice for responding to a valid request by the Data Protection Manager.

28.20 Where we process a large quantity of information about an individual, we may need to ask the individual to specify the information or processing activities to which the request relates.

©TransitionLaw2025

28.21 While it is not a requirement under UK GDPR that an individual must make a DSAR in writing, it is helpful for the Company if they do so. Individuals should therefore be encouraged to use the email address provided in this document.

28.22 We will not usually charge a fee for responding to a data subject access request. We may, however, charge a reasonable fee (based on the administrative cost of providing the information) for responding to a request:

28.22.1 that is manifestly unfounded or excessive, e.g. repetitive; or

28.22.2 for further copies of the same information.

Identifying the data subject

28.23 Before responding to a data subject access request, the **Data Protection Manager** will take reasonable steps to verify the identity of the person making the request.

28.24 We will not retain personal data, e.g. relating to former employees for the sole purpose of being able to react to potential data subject access requests in the future.

28.25 If we have doubts as to the identity of the person making the data subject access request, we may ask for additional information to confirm their identity.

28.26 Typically we will request a copy of the individual's driving licence or passport to enable us to establish their identity and signature (which should be compared to the signature on the data subject access request and any signature we already hold for the individual). We may also ask for a recent utility bill (or equivalent) to verify the individual's identity and address.

28.27 If, having requested additional information, we are still not in a position to identify the data subject, we may refuse to act on a data subject access request.

Refusing to respond to a request

28.28 We may refuse to act on a data subject access request where:

28.28.1 even after requesting additional information, we are not in a position to identify the individual making the data subject access request;

28.28.2 requests from an individual are manifestly unfounded or excessive, e.g. because of their repetitive character.

28.29 If we intend to refuse to act on a data subject access request, we will inform the individual, within one month of receiving the individual’s request:

28.29.1 of the reason(s) why we are not taking action; and

28.29.2 that they have the right to complain to the ICO and seek a judicial remedy.

Time limit for responding to a request

28.30 Once a data subject access request is received, the Company must provide the information requested without delay and at the latest within one month of receiving the request.

©TransitionLaw2025

28.31 Therefore a note of when request was received and when the time limit will end must be kept by the **Data Protection Manager** and recorded in the data protection register.

28.32 If a data subject access request is complex or the data subject has made numerous requests, the Company:

28.32.1 may extend the period of compliance by a further two months; and

28.32.2 must inform the individual of the extension within one month of the receipt of the request and explain why the extension is necessary.

Information to be provided in response to a request

28.33 The individual is entitled to receive access to the personal data we process about the individual and the following information:

28.33.1 the purposes for which we process the data;

28.33.2 the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;

28.33.3 where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;

28.33.4 the fact that the individual has the right:

(a) to request that the Company rectifies, erases or restricts the processing of the individual's personal data; or

(b) to object to its processing;

(c) to lodge a complaint with the ICO;

28.33.5 where the personal data has not been collected from the individual, any information available regarding the source of the data;

28.33.6 any automated decision we have taken about the individual, together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

28.34 The information referred to above should be provided:

28.34.1 in a way that is concise, transparent, easy to understand and easy to access;

28.34.2 using clear and plain language, with any technical terms, abbreviations or codes explained;

28.34.3 in writing;

28.34.4 in a commonly-used electronic format, if the data subject access request was made electronically, unless otherwise requested by the individual.

©TransitionLaw2025

Automated decision-making

28.35 If the data subject access request specifically asks for information about the logic behind any automated decision that we have taken in relation to important matters relating to the individual (e.g. performance at work, creditworthiness, reliability or conduct), we must provide a description of the logic involved in that automated decision, subject to the following conditions:

28.35.1 the automated decision must have constituted the sole basis for the decision. For example, an application for credit which is conducted without any human intervention, other than to complete the application form, could be a decision which is taken solely by automatic means. However, if there is any element of human discretion as to whether or not to grant the credit, the decision would cease to be wholly automated and the individual would not be entitled to a description of the logic;

28.35.2 in providing a description of the logic we are not required to reveal any information which constitutes a trade secret.

28.36 If the Company carries out automated decision-making in relation to an individual, the data subject access request may include a request:

28.36.1 for information relating to the automated decision;

28.36.2 for human intervention on the part of the Company, i.e. to ask that an individual with the authority and competence to change the decision should review the automated decision, considering all the available data;

28.36.3 to express their point of view on the automated decision; and/or

28.36.4 to contest the automated decision.

If such a request is received, the **Data Protection Manager** will ensure that it is dealt with in accordance with UK GDPR and other relevant legislation and guidance.

How to locate information

28.37 The personal data we need to provide in response to a data subject access request may be located in several electronic and manual filing systems or on those of data processors or other third parties. Consequently, it is important to identify at the outset the type of information requested so that the search can be focused.

28.38 Depending on the type of information requested, a search may be needed in all or some of the following media:

28.38.1 electronic systems, e.g. databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;

28.38.2 manual filing systems in which personal data are accessible according to specific criteria, e.g. chronologically ordered sets of manual records containing personal data;

28.38.3 data systems held externally by our data processors e.g. external payroll service providers;

©TransitionLaw2025

28.38.4 private devices used by employees and others;

28.38.5 occupational health records;

28.38.6 pensions data;

28.38.7 share scheme information;

28.38.8 insurance benefit information;

The above systems should be searched using the individual's name, employee number, customer account number or other personal identifier as a search determinant as applicable.

What is personal data?

28.39 Once you have carried out the search and gathered the results, you will need to select the information to be supplied in response to the data subject access request. The individual is only entitled to access to information which constitutes the individual's personal data.

28.40 Personal data is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, eg their name, identification number, location data or online identifier. It may also include personal data that has been pseudonymised (eg key-coded), depending on how difficult it is to attribute the pseudonym to a particular individual.

Requests made by third parties on behalf of the individual

28.41 Occasionally we may receive a request for data subject access by a third party (an 'agent') acting on behalf of an individual.

28.42 Such agents may include parents, guardians, legal representatives and those acting under a power of attorney or other legal authority. The agent must provide sufficient evidence that the agent is authorised to act on behalf of the individual.

Exemptions to the right of subject access

28.43 In certain circumstances we may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention:

28.44 We do not have to disclose any personal data which we are processing for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

28.45 This is not an absolute exemption. It only applies to the extent to which the giving of subject access would be likely to prejudice any of these purposes. We are still required to provide as much of the personal data as we able to. For example, if the disclosure of the personal data could alert the individual to the fact that they are being investigated for an illegal activity (ie by us or by the police) then we do not have to disclose the data since the disclosure would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

©TransitionLaw2025

Protection of rights of others:

28.46 We do not have to disclose personal data to the extent that doing so would involve disclosing information which identifies another individual, unless:

28.46.1 that other individual has consented to the disclosure of the information to the individual making the request; or

28.46.2 it is reasonable to disclose the information to the individual making the request without the other individual's consent, having regard to:

(a) the type of information that would be disclosed;

(b) any duty of confidentiality owed to the other individual;

(c) any steps taken by the controller with a view to seeking the consent of the other individual;

(d) whether the other individual is capable of giving consent; and

(e) any express refusal of consent by the other individual.

Confidential references:

28.47 We do not have to disclose any confidential references that we have given to third parties for the purpose of actual or prospective:

28.47.1 education, training or employment of the individual;

28.47.2 appointment of the individual to any office; or

28.47.3 provision by the individual of any service

NB: This exemption does not apply to confidential references that we receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (ie the person giving the reference), which means you must consider the rules regarding disclosure of third-party data before disclosing the reference.

Legal professional privilege:

28.48 We do not have to disclose any personal data which are subject to legal professional privilege. There are two types of legal professional privilege:

28.48.1 'legal advice privilege', which covers confidential communications between the Company and its professional legal advisers for the purpose of seeking or obtaining legal advice;

28.48.2 'litigation privilege', which covers confidential communications between the Company and its professional legal advisers or a third party where litigation is contemplated or in progress.

If you think the legal professional privilege exemption could apply to the personal data that have been requested, or are in any way uncertain as to whether it might apply, you should refer the matter to our legal advisers for further advice.

©TransitionLaw2025

Corporate finance:

28.49 We do not have to disclose any personal data which we process for the purposes of, or in connection with, a corporate finance service if:

28.49.1 disclosing the personal data would be likely to affect the price of an instrument; or

28.49.2 disclosing the personal data would have a prejudicial effect on the orderly functioning of financial markets or the efficient allocation of capital within the economy and we believe that it could affect a person's decision:

(a) whether to deal in, subscribe for or issue an instrument;

(b) whether to act in a way likely to have an effect on a business activity, eg on the industrial strategy of a person, the capital structure of an undertaking or the legal or beneficial ownership of a business or asset.

Management forecasting:

28.50 We do not have to disclose any personal data which we process for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity. Examples of management forecasting and planning activities include staff relocations, redundancies, succession planning, promotions and demotions.

28.50.1 This exemption must be considered on a case-by-case basis and must only be applied to the extent to which disclosing the personal data would be likely to prejudice the conduct of that business or activity.

Negotiations:

28.51 We do not have to disclose any personal data consisting of records of our intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations. For example, if the HR department is negotiating with an employee in order to agree the terms of a redundancy package and the employee makes a data subject access request, the HR department can legitimately withhold giving access to information which would prejudice those redundancy negotiations.

28.51.1 We must, however, disclose all other personal data relating to the individual unless those other personal data are also exempt from disclosure.

Deleting personal data in the normal course of business

28.52 The information that we are required to supply in response to a data subject access request must be supplied by reference to the data in question at the time the request was received.

28.53 However, as we have one month in which to respond and we are generally unlikely to respond on the same day as we receive the request, we are allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data are supplied if such amendment or deletion would have been made regardless of the receipt of the data subject access request.

©TransitionLaw2025

28.54 We are, therefore, allowed to carry out regular housekeeping activities even if this means that we delete or amend personal data after the receipt of a data subject access request. What we are not allowed to do is amend or delete data because we do not want to supply the data.

Consequences of failing to comply with this policy

28.55 The Company takes compliance with this policy very seriously. If we fail to comply with a subject access request or fail to provide access to all the personal data requested or fail to respond within the one-month time period, we will be in breach of GDPR and other relevant legislation. This may have several consequences:

28.55.1 it may put at risk the individual(s) whose personal information is being processed;

28.55.2 the individual may complain to the ICO and this may lead the ICO to investigate the complaint. If we are found to be in breach, enforcement action could follow, which carries the risk of significant civil and criminal sanctions for the Company and, in some circumstances, for the individual responsible for the breach;

28.55.3 if an individual has suffered damage, or damage and distress, as a result of our breach of UK GDPR or other relevant legislation, the individual may take us to court and claim damages from us; and

28.55.4 a court may order us to comply with the subject access request if we are found not to have complied with our obligations under UK GDPR and other relevant legislation.

28.56 Any questions regarding this Policy should be addressed to the **Data Protection Manager**.

29 Data Breach Policy

29.1 We accept the Information Commissioners Office definition of a data breach as follows:

29.2 “A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.”

29.3 We have determined a policy to comply with Data Breaches in the Company as follows:

29.4 A data breach may take many different forms, for example:

29.4.1 loss or theft of data or equipment on which personal data is stored;

29.4.2 unauthorised access to or use of personal data either by a member of staff or third party;

29.4.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

29.4.4 human error, such as accidental deletion or alteration of data;

29.4.5 unforeseen circumstances, such as a fire or flood;

©TransitionLaw2025

29.4.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

29.4.7 'blagging' offences, where data is obtained by deceiving the organisation which holds it.

29.5 Details of the breach will be notified to or come to the notice of our **Data Protection Manager** who will begin an investigation into the breach to determine:-

29.5.1 Its existence – has there in fact been a breach.

29.5.2 Its extent – how much data has been breached.

29.5.3 Its consequences – the consequences dictate the next actions as described below.

29.6 The **Data Protection Manager** will inform the ICO as soon as practicable and in any event within 72 hours if the breach is likely to result in a risk to the rights and freedoms of individuals or could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

29.7 In addition to the provisions above the **Data Protection Manager** is responsible for notifying each of the data subjects concerned directly, if a breach is likely to result in a high risk to the rights and freedoms of individuals.

29.8 If a minor data breach has occurred which does not require notification to the Regulator the **Data Protection Manager** will record the incident in Data Protection Register along with the justification for not reporting it.

29.9 All data breaches whether reportable or not will be recorded in our records to:

29.9.1 Demonstrate our response to the incident.

29.9.2 Comply with our record keeping responsibilities under UK GDPR.

29.9.3 Maintain a satisfactory record of our actions for future reference.

©TransitionLaw2025

Business Compliance Document

PART FIVE of FIVE

LEGITIMATE INTEREST
&
UPDATES POLICIES

©TransitionLaw2025

Policies requiring a Legitimate Interest Assessment

30 Business Marketing

30.1 We do not engage in Direct Marketing activity for the business.

30.2 We do not make use of Automated calling systems, Unsolicited live calls or Electronic Communications including Emails, Text messages, Telephone Calls, MMS or Faxes.

30.3 We may conduct Marketing activity through the use of non directed advertising in newspapers, periodicals, leaflets and similar.

30.4 We are familiar with the provisions of the Privacy & Electronic Communications Regulations (PECR).

30.5 The PECR Regulations apply to our Marketing effort in the respect of contacting prospective clients whose details have been passed to us by third parties.

30.5.1 We process such information using the lawful basis of Consent and confirm with the providing third party that consent has been lawfully obtained and we are named as the recipient of the Personal Data in such Consent.

30.6 We may conduct unsolicited Marketing to the published business contact data for incorporated firms who do not fall within the definition of a personal subscriber under PECR.

30.7 We maintain our own 'do not call' list of people who may not be on any official list but have informed us they do not wish to receive marketing calls from ourselves.

30.8 We may receive Personal Data from third parties. We process such information using the lawful basis of Consent and confirm with the providing third party that consent has been lawfully obtained and we are named as the recipient of the Personal Data in such Consent.

31 Video Conferencing Policy

General

31.1 We use 3rd party proprietary video conferencing facilities within our business activity, which are able to record the conversations and presentations which occur during their use.

31.2 We understand that the participants of these conversations should be made aware that we are processing their Personal Data.

31.3 Where Video conferencing conversations are recorded and kept by us this data may be subject of a Data Subject Access Request. (DSAR)

31.4 We do not generally record and keep the conversations but when we do so the data and its security will be in dealt with in accordance with this Privacy policy.

31.5 A Legitimate Interests Assessment was conducted regarding video conferencing and is reproduced in this document.

31.6 This Policy has been established in accordance with the determinations of our Data Audit and the published guidance of the UK National Cyber Security Centre. (NCSC) on Video Conferencing and Cloud security.

©TransitionLaw2025

31.7 We will only use the Video Conferencing Application Platforms (the Platform) which are from time to time approved by the Management.

31.8 The Security and Privacy settings on the Platform will be checked and adjusted to ensure the safety of participants to the call.

31.9 The choice of platform will be reviewed at least annually during the Privacy review or sooner if issues are reported to the **Data Protection Manager**.

Phishing

31.10 We are aware of the practice of Phishing during video conference calls. Phishing may be defined as follows: 'Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.'

31.11 Caution will be used when engaged in video conference calling especially in the use of any 'Live Chat' features to reduce the opportunities for Phishing.

31.12 Participants will not be allowed to share external links during the call without the express permission of the Moderator.

31.13 All Participants will be warned regarding the dangers of Phishing, clicking unknown links etc at the commencement of a call.

The Platform

31.14 The Video Conference Platform will be approved by the Management before use.

31.15 The latest software version must be checked for and downloaded prior to each use of the platform.

31.16 Consideration will be given to any 'paid for' version of the Platform if such a version exists and if it provides greater security and Privacy for the participants.

Passwords

31.17 Every use of the Platform will be controlled by the use of a Password to access any individual Video Conference call.

31.18 To reduce the risk of phishing and or deliberate interference or corruption of the process, when the call is either open to the public or has more than 5 separate participants, consideration will be given to using individual passwords for each participant.

Storage and Uploading of Video Conferencing

31.19 Video Conference recording facilities are available on most platforms.

31.20 We understand the image of a participant on a Video Conference call is Personal Data and can be subject to a Data Access request.

31.21 Where we intend to keep recordings of Video Conference calls this will be notified to participants at the start of the call to provide an opportunity for them to 'Opt out' by closing their video link and remaining on the call using audio only or by leaving the call altogether.

©TransitionLaw2025

Video Conferencing Applications – Legitimate Interest Assessment

31.22 We use 3rd party proprietary video conferencing facilities within our business activity, which are able to record the conversations and presentations which occur during their use.

31.23 We understand that the participants of these conversations should be made aware that we are processing their Personal Data.

31.24 Where Video conferencing conversations are recorded and kept by us this data may be subject of a Data Subject Access Request. (DSAR)

31.25 We do not generally record and keep the conversations but when we do so the data and its security will be in dealt with in accordance with this Privacy policy.

31.26 A Legitimate Interests Assessment was conducted by Us and is reproduced below:

31.27 In the course of our primary business activity we will gather Personal Data due to the use of Video Conferencing applications.

31.28 We wish to use Video Conferencing applications to facilitate efficient and speedy communications between interested parties engaged upon or connected to our business activity. These parties are often in disparate locations which makes direct communication without using technology virtually impossible.

31.29 We derive a substantial benefit in terms of a reduction in time spent travelling using a video conferencing platform.

31.30 The video conferencing platform is a 3rd party proprietary application which is publicly available and confirms to the prevailing Privacy regulations in and of itself.

31.31 Our use of the Platform will be within the manufacturer's suggested operating procedures.

31.31.1 If we did not process the data by video conferencing the alternative would be to use traditional telecommunications which has fewer features and is not satisfactory in terms of content delivery when visual images are required.

31.31.2 The software we use is compliant with the UK Government's National Cyber Security Centre (NCSC) guidelines for Video Conferencing.

31.31.3 We maintain a high level of data privacy standards including Data Processing agreements where necessary with our primary business partners.

31.31.4 We will not always record the video conference call but if we do, any Personal Data processed will not be of the kind to cause any ethical issues and will be dealt with in line with our robust and fully operational UK GDPR privacy policies and systems.

31.32 Video Conferencing and the use of images both of the participants and with reference to non Personal Data information such as charts, graphs, photographs etc is the only way to achieve the purpose and transmit the information necessary for the successful completion of the agenda of the call.

31.33 The use of Video Conference calling is a proportionate methodology to fulfil our communication needs.

©TransitionLaw2025

31.34 Mulltiple location communication is not possible without some form of technology and the transmission of information, especially graphical and photographic information is not possible using traditional telecommunications.

31.35 Receiving and processing Personal Data during Video Conference calling is a well established medium for the transference of data.

31.36 All participants on the call will have received notification that we will be processing their data.

31.37 All participants in the call will have opted in to the 3rd party application provider's Terms and Conditions.

31.38 All participants in the call will be adults.

31.39 Video conferencing is not an unusual method of processing and We do not expect anyone to object to the processing of their data in this way.

31.40 We recognise that any data we retain from the video conference can form the basis of a Subject Access Request which can be made to us under our Policy in this document should a data subject have any concerns.

31.41 The Legitimate Interest Assessment Test determined the following:

31.42 Following the assessment, it was decided that there was no infringement of the UK GDPR or the rights of the individual participants in our use of a Video Conferencing Application.

31.43 The legal basis for the processing was established as being in our Legitimate Interests for the following purposes:

31.44 To facilitate efficient business video and telecommunications.

31.45 To protect the safety of our employees and participants on the call from unnecessary real world travelling.

31.46 To support our primary business objectives.

32 CCTV

32.1 We do not use Closed Circuit Television equipment (CCTV) within our business activity.

32.2 If this policy changes, or such a change is made or planned to be made We will complete a detailed Data Processing Impact Assessment and Legitimate Interest Assessment and update this policy statement accordingly.

33 Dashcams

33.1 We do not make use of Dashcam equipment within our business operation.

33.2 If this policy changes, or such a change is made or planned to be made We will complete a detailed Data Processing Impact Assessment and Legitimate Interest Assessment and update this policy statement accordingly

©TransitionLaw2025

34 Review and Updating

34.1 We recognise the developing nature of Data Processing legislation and procedures.

34.2 We have established a regular system for review and updating as required.

34.3 Our **Data Protection Manager** is responsible for arranging reviews of our systems and staff training in line with our established training schedule.

34.4 We intend to create a robust system of Data Protection by design. We will conduct a Data/Information Audit on a regular basis as required by the regulations and record any updates to these policies.

34.5 A Data Audit will be conducted:

34.5.1 Regularly and in any event at least Annually.

34.5.2 When changes to procedures or processes warrant a Data Processing Impact Assessment (DPIA)

34.5.3 When any other relevant changes are required

34.5.4 The Data Protection staff training schedule is established as follows:

(a) Induction – On appointment or re-appointment.

(b) Ongoing - On a rolling six monthly basis of knowledge checks and reminders.

(c) Updating – As required consequent to changing and developing rules and procedures.

34.6 Our Data Processing contact has been authorised to make enquiries of our Legal advisors, if required, in the event of any queries beyond their existing understanding and knowledge.

Policy Currency

34.7 Policy Active from: 1 February 2025

34.8 Update required by: 1 February 2026

Date	Update Required	Reason for Revision	Applicable to	Signed by DP Manager	Print Name
1.2.25	Policy updates	UK GDPR/DPA 18	All Staff		Mr Andrea Facchini

©TransitionLaw2025